



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
-----------------	-------------	----------------------	---------------------	------------------

10/820,980

04/07/2004

Amol Khare

50325-0892

9036

29989

7590

09/24/2008

HICKMAN PALERMO TRUONG & BECKER, LLP
2055 GATEWAY PLACE
SUITE 550
SAN JOSE, CA 95110

EXAMINER

CHEN, SHIN HON

ART UNIT

PAPER NUMBER

2131

MAIL DATE

DELIVERY MODE

09/24/2008

PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No. 10/820,980	Applicant(s) KHARE ET AL.	
	Examiner SHIN-HON CHEN	Art Unit 2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☒ Responsive to communication(s) filed on 30 June 2008.
- 2a) ☒ This action is **FINAL**. 2b) ☐ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-36 is/are pending in the application.
- 4a) Of the above claim(s) _____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) _____ is/are allowed.
- 6) ☒ Claim(s) 1-36 is/are rejected.
- 7) ☒ Claim(s) 18 is/are objected to.
- 8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☒ The drawing(s) filed on 07 April 2004 is/are: a) ☒ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
 2. ☐ Certified copies of the priority documents have been received in Application No. _____.
 3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- | | |
|--|---|
| 1) <input type="checkbox"/> Notice of References Cited (PTO-892) | 4) <input type="checkbox"/> Interview Summary (PTO-413) |
| 2) <input type="checkbox"/> Notice of Draftsperson's Patent Drawing Review (PTO-948) | Paper No(s)/Mail Date. _____ |
| 3) <input type="checkbox"/> Information Disclosure Statement(s) (PTO/SB/08) | 5) <input type="checkbox"/> Notice of Informal Patent Application |
| Paper No(s)/Mail Date _____ | 6) <input type="checkbox"/> Other: _____ |

DETAILED ACTION

1. Claims 1-36 have been examined.

Claim Rejections - 35 USC § 112

2. Claims 1-36 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention.

The newly amended claims 1-36 recite “a packet sequence value from the portion of the header that is included within the data field within the ICMP packet”. Applicant asserts that the amendment does not add any new matter to this application by pointing to Paragraph [0012] and [0020] for support. However, the Specification discloses that the packet sequence value is obtained from the header, not the data field (Specification: page 6 paragraph [0020] line 6). On the other hand, although paragraph [0012] states that RFC 792 discloses that some ICMP error packets comprise a copy of the IP header of the original packet, it does not constitute sufficient description reasonably convey that applicant had possession of the claimed invention. Therefore, the examiner will examine claims 1-36 will considering the limitations that are subject to this rejection.

Art Unit: 2131

Claim Objections

3. Claim 18 is objected to because of the following informalities: Claim 18 discloses a nonvolatile or volatile computer-readable medium, which includes carrier wave as disclosed in the specification (Specification: [0059]). Applicant is advised to amend the claim to “ a computer-readable **storage** medium”. Appropriate correction is required.

Claim Rejections - 35 USC § 103

4. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

5. Claims 1-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Talpade et al. U.S. Pub. No. 20040148520 (hereinafter Talpade) in view of Fan et al. U.S. Pat. No. 6219706 (hereinafter Fan).

6. As per claim 1, Talpade discloses a method of preventing an attack on a network, the method comprising the computer-implemented steps of:

receiving an ICMP packet, wherein a data field within the ICMP packet includes a portion of a header associated with a connection in a connection-oriented transport protocol (Talpade: [0020] lines 4-5 and lines 13-15: analyze packet header for packet filtering for ICMP packet based on range of valid values of various packet header fields);

Art Unit: 2131

and responding to the ICMP packet by updating a parameter associated with the transport protocol connection only if the packet field value is determined to be valid (Talpad: [0017] lines 27-30: forwarding traffic/updating parameter associated with protocol connection if packet is not DDoS packet/the packet value is valid).

Talpad does not explicitly disclose wherein the portion of the header includes a packet sequence value associated with the connection; obtaining a packet sequence value from the header; determining if the packet sequence value is valid; and responding to the ICMP packet by updating a parameter value associated with the transport protocol connection only if the packet sequence value is determined to be valid.

However, Fan discloses filtering packets based on the sequence number presented in the header portion of a packet and update the current session state if sequence value is valid (Fan: column 10 lines 27-51: using packet values to filter DDoS packets). It would have been obvious to one having ordinary skill in the art to utilize the sequence number contained in the connection-oriented packet into the field value of the ICMP packet because they are analogous art used to control DoS attack. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Fan within the system of Talpad because it allows packet filter to analyze invalid range of value presented in header for filtering purposes.

7. As per claim 2, Talpad as modified discloses the method of claim 1. Talpad as modified further discloses wherein the step of receiving an ICMP packet comprises receiving an

Art Unit: 2131

ICMP packet that includes a copy of a TCP header associated with a TCP connection (Fan: column 10 lines 27-51). Same rationale applies here as above in rejecting claim 1.

8. As per claim 3, Talpade as modified discloses the method of claim 1. Talpade as modified further discloses wherein the step of receiving an ICMP packet comprises receiving an ICMP "endpoint unreachable" error packet (Talpade: [0006]: error packets in denial of service attack).

9. As per claim 4, Talpade as modified discloses the method of claim 1. Talpade as modified further discloses wherein the step of receiving an ICMP packet comprises receiving an ICMP packet that specifies that fragmentation is needed (Talpade: [0020] lines 4-6: ICMP messages).

10. As per claim 5, Talpade as modified discloses the method of claim 1. Talpade as modified further discloses wherein the step of authenticating the ICMP packet by determining if the packet sequence value is valid comprises determining if the packet sequence value is within a range of packet sequence values that are allowed by the transport protocol for the connection (Fan: column 10 lines 27-51).

11. As per claim 6, Talpade as modified discloses the method of claim 1. Talpade as modified further discloses wherein the step of authenticating the ICMP packet by determining if the packet sequence value is valid comprises determining if the packet sequence value is within a

Art Unit: 2131

range of sent but unacknowledged TCP packet sequence values for the connection (Fan: column 10 lines 27-51).

12. As per claim 7, Talpade as modified discloses the method of claim 1. Talpade as modified further discloses wherein the step of authenticating the ICMP packet by determining if the packet sequence value is valid comprises determining if the packet sequence value is exactly equal to one or more sequence values of one or more packets that are then-currently stored in a TCP re-transmission buffer, starting at a sequence value of a previously sent segment that resulted in receiving the ICMP packet (Fan: column 10 lines 35-41).

13. As per claim 8, Talpade as modified discloses the method of claim 1. Talpade as modified further discloses wherein the steps are performed in a router acting as a TCP endpoint node (Talpade: [0020]: sensor/firewall).

14. As per claim 9, Talpade as modified discloses the method of claim 1. Talpade as modified further discloses wherein the steps are performed in a firewall device (Talpade: [0020]: packet filtering device/firewall; Fan: column 10 lines 27-51: firewall/packet filter).

15. As per claim 10, Talpade discloses a method of preventing an attack on a network, the method comprising the computer-implemented steps of:

receiving, at a TCP endpoint node in a TCP/IP packet-switched network (Talpade: [0020] line 1-5: monitor all traffic entering customer network that includes TCP/IP protocol), an ICMP

Art Unit: 2131

packet, wherein a data field within the ICMP packet includes a portion of a header associated with a connection in a connection-oriented transport protocol (Talpade: [0020] lines 4-5 and lines 13-15: analyze packet header for packet filtering for ICMP packet based on range of valid values of various packet header fields);

and responding to the ICMP packet by updating a parameter associated with the transport protocol connection only if the packet field value is determined to be valid (Talpad: [0017] lines 27-30: forwarding traffic/updating parameter associated with protocol connection if packet is not DDoS packet/the packet value is valid).

Talpade does not explicitly disclose wherein the portion of the header includes a packet sequence value associated with the connection; obtaining a packet sequence value from the header; determining if the packet sequence value is valid; and responding to the ICMP packet by updating a parameter value associated with the transport protocol connection only if the packet sequence value is determined to be valid.

However, Fan discloses filtering packets based on the sequence number presented in the header portion of a packet and update the current session state if sequence value is valid (Fan: column 10 lines 27-51: using packet values to filter DDoS packets). It would have been obvious to one having ordinary skill in the art to utilize the sequence number contained in the connection-oriented packet into the field value of the ICMP packet because they are analogous art used to control DoS attack. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Fan within the system of Talpade because it allows packet filter to analyze invalid range of value presented in header for filtering purposes.

Art Unit: 2131

Talpade as modified does not explicitly disclose updating MTU value associated with the TCP connection. However, Talpade discloses forwarding traffic if the packet value is valid (Talpade: [0017] lines 27-30) and it would have obvious to one having ordinary skill in the art to take different measures to allow traffic including, but not limited to, updating MTU value to increase transmission rate to allow traffic.

16. As per claim 11, Talpade as modified discloses the method of claim 10. Talpade as modified further discloses wherein the step of receiving an ICMP packet comprises receiving an ICMP "endpoint unreachable" error packet (Talpade: [0006]: error packets in denial of service attack).

17. As per claim 12, Talpade as modified discloses the method of claim 10. Talpade as modified further discloses wherein the step of receiving an ICMP packet comprises receiving an ICMP packet that specifies that fragmentation is needed (Talpade: [0020] lines 4-6: ICMP messages).

18. As per claim 13, Talpade as modified discloses the method of claim 10. Talpade as modified further discloses wherein the step of authenticating the ICMP packet by determining if the packet sequence value is valid comprises determining if the packet sequence value is within a range of packet sequence values that are allowed by the transport protocol for the connection (Fan: column 10 lines 27-51).

Art Unit: 2131

19. As per claim 14, Talpade as modified discloses the method of claim 10. Talpade as modified further discloses wherein the step of authenticating the ICMP packet by determining if the packet sequence value is valid comprises determining if the packet sequence value is within a range of sent but unacknowledged TCP packet sequence values for the connection (Fan: column 10 lines 27-51).

20. As per claim 15, Talpade as modified discloses the method of claim 10. Talpade as modified further discloses wherein the step of authenticating the ICMP packet by determining if the packet sequence value is valid comprises determining if the packet sequence value is exactly equal to one or more sequence values of one or more packets that are then-currently stored in a TCP re-transmission buffer, starting at a sequence value of a previously sent segment that resulted in receiving the ICMP packet (Fan: column 10 lines 35-41).

21. As per claim 16, Talpade as modified discloses the method of claim 10. Talpade as modified further discloses wherein the steps are performed in a router acting as a TCP endpoint node (Talpade: [0020]: sensor/firewall).

22. As per claim 17, Talpade as modified discloses the method of claim 10. Talpade as modified further discloses wherein the steps are performed in a firewall device (Talpade: [0020]: packet filtering device/firewall; Fan: column 10 lines 27-51: firewall/packet filter).

Art Unit: 2131

23. As per claim 18, Talpade discloses a volatile or nonvolatile computer-readable medium carrying one or more sequences of instruction, which instructions, when executed by one or more processors, cause the one or more processors to perform the steps of:

receiving an ICMP packet, wherein a data field within the ICMP packet includes a portion of a header associated with a connection in a connection-oriented transport protocol (Talpade: [0020] lines 4-5 and lines 13-15: analyze packet header for packet filtering for ICMP packet based on range of valid values of various packet header fields);

and responding to the ICMP packet by updating a parameter associated with the transport protocol connection only if the packet field value is determined to be valid (Talpade: [0017] lines 27-30: forwarding traffic/updating parameter associated with protocol connection if packet is not DDoS packet/the packet value is valid).

Talpade does not explicitly disclose wherein the portion of the header includes a packet sequence value associated with the connection; obtaining a packet sequence value from the header; determining if the packet sequence value is valid; and responding to the ICMP packet by updating a parameter value associated with the transport protocol connection only if the packet sequence value is determined to be valid.

However, Fan discloses filtering packets based on the sequence number presented in the header portion of a packet and update the current session state if sequence value is valid (Fan: column 10 lines 27-51: using packet values to filter DDoS packets). It would have been obvious to one having ordinary skill in the art to utilize the sequence number contained in the connection-oriented packet into the field value of the ICMP packet because they are analogous art used to control DoS attack. Therefore, it would have been obvious to one having ordinary skill in the art

Art Unit: 2131

at the time of applicant's invention to combine the teachings of Fan within the system of Talpade because it allows packet filter to analyze invalid range of value presented in header for filtering purposes.

24. As per claim 19, Talpade discloses an apparatus for preventing an attack on a network, comprising:

means for receiving an ICMP packet, wherein a data field within the ICMP packet includes a portion of a header associated with a connection in a connection-oriented transport protocol (Talpade: [0020] lines 4-5 and lines 13-15: analyze packet header for packet filtering for ICMP packet based on range of valid values of various packet header fields);

and means for responding to the ICMP packet by updating a parameter associated with the transport protocol connection only if the packet filed value is determined to be valid (Talpad: [0017] lines 27-30: forwarding traffic/updating parameter associated with protocol connection if packet is not DDoS packet/the packet value is valid).

Talpade does not explicitly disclose wherein the portion of the header includes a packet sequence value associated with the connection; means for obtaining a packet sequence value from the header; means for determining if the packet sequence value is valid; and responding to the ICMP packet by updating a parameter value associated with the transport protocol connection only if the packet sequence value is determined to be valid.

However, Fan discloses filtering packets based on the sequence number presented in the header portion of a packet and update the current session state if sequence value is valid (Fan: column 10 lines 27-51: using packet values to filter DDoS packets). It would have been obvious

Art Unit: 2131

to one having ordinary skill in the art to utilize the sequence number contained in the connection-oriented packet into the field value of the ICMP packet because they are analogous art used to control DoS attack. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Fan within the system of Talpade because it allows packet filter to analyze invalid range of value presented in header for filtering purposes.

25. As per claim 20, Talpade as modified discloses the apparatus of claim 19. Talpade as modified further discloses wherein the step of receiving an ICMP packet comprises receiving an ICMP packet that includes a copy of a TCP header associated with a TCP connection (Fan: column 10 lines 27-51). Same rationale applies here as above in rejecting claim 1.

26. As per claim 21, Talpade as modified discloses the apparatus of claim 19. Talpade as modified further discloses wherein the step of receiving an ICMP packet comprises receiving an ICMP "endpoint unreachable" error packet (Talpade: [0006]: error packets in denial of service attack).

27. As per claim 22, Talpade as modified discloses the apparatus of claim 19. Talpade as modified further discloses wherein the step of receiving an ICMP packet comprises receiving an ICMP packet that specifies that fragmentation is needed (Talpade: [0020] lines 4-6: ICMP messages).

Art Unit: 2131

28. As per claim 23, Talpade as modified discloses the apparatus of claim 19. Talpade as modified further discloses wherein the step of authenticating the ICMP packet by determining if the packet sequence value is valid comprises determining if the packet sequence value is within a range of packet sequence values that are allowed by the transport protocol for the connection (Fan: column 10 lines 27-51).

29. As per claim 24, Talpade as modified discloses the apparatus of claim 19. Talpade as modified further discloses wherein the step of authenticating the ICMP packet by determining if the packet sequence value is valid comprises determining if the packet sequence value is within a range of sent but unacknowledged TCP packet sequence values for the connection (Fan: column 10 lines 27-51).

30. As per claim 25, Talpade as modified discloses the apparatus of claim 19. Talpade as modified further discloses wherein the step of authenticating the ICMP packet by determining if the packet sequence value is valid comprises determining if the packet sequence value is exactly equal to one or more sequence values of one or more packets that are then-currently stored in a TCP re-transmission buffer, starting at a sequence value of a previously sent segment that resulted in receiving the ICMP packet (Fan: column 10 lines 35-41).

31. As per claim 26, Talpade as modified discloses the apparatus of claim 19. Talpade as modified further discloses wherein the steps are performed in a router acting as a TCP endpoint node (Talpade: [0020]: sensor/firewall).

32. As per claim 27, Talpade as modified discloses the apparatus of claim 19. Talpade as modified further discloses wherein the steps are performed in a firewall device (Talpade: [0020]: packet filtering device/firewall; Fan: column 10 lines 27-51: firewall/packet filter).

33. As per claim 28, Talpade discloses a network element, comprising:

- a network interface that is coupled to a data network for receiving one or more packet flows therefrom (Talpade: figure 2: filter router 230);
- a processor (Talpade: figure 2: filter router 230 contains processor);
- on or more stored sequence s of instruction which, when executed by the processor, cause the processor to perform the steps of:
 - receiving an ICMP packet, wherein a data field within the ICMP packet includes a portion of a header associated with a connection in a connection-oriented transport protocol (Talpade: [0020] lines 4-5 and lines 13-15: analyze packet header for packet filtering for ICMP packet based on range of valid values of various packet header fields);
 - responding to the ICMP packet by updating a parameter associated with the transport protocol connection only if the packet filed value is determined to be valid (Talpade: [0017] lines 27-30: forwarding traffic/updating parameter associated with protocol connection if packet is not DDoS packet/the packet value is valid).

Talpade does not explicitly disclose wherein the portion of the header includes a packet sequence value associated with the connection; means for obtaining a packet sequence value from the header; means for determining if the packet sequence value is valid; and responding to

Art Unit: 2131

the ICMP packet by updating a parameter value associated with the transport protocol connection only if the packet sequence value is determined to be valid.

However, Fan discloses filtering packets based on the sequence number presented in the header portion of a packet and update the current session state if sequence value is valid (Fan: column 10 lines 27-51: using packet values to filter DDoS packets). It would have been obvious to one having ordinary skill in the art to utilize the sequence number contained in the connection-oriented packet into the field value of the ICMP packet because they are analogous art used to control DoS attack. Therefore, it would have been obvious to one having ordinary skill in the art at the time of applicant's invention to combine the teachings of Fan within the system of Talpade because it allows packet filter to analyze invalid range of value presented in header for filtering purposes.

34. As per claim 29, Talpade as modified discloses the network element of claim 28. Talpade as modified further discloses wherein the step of receiving an ICMP packet comprises receiving an ICMP packet that includes a copy of a TCP header associated with a TCP connection (Fan: column 10 lines 27-51). Same rationale applies here as above in rejecting claim 1.

35. As per claim 30, Talpade as modified discloses the network element of claim 28. Talpade as modified further discloses wherein the step of receiving an ICMP packet comprises receiving an ICMP "endpoint unreachable" error packet (Talpade: [0006]: error packets in denial of service attack).

Art Unit: 2131

36. As per claim 31, Talpade as modified discloses the network element of claim 28. Talpade as modified further discloses wherein the step of receiving an ICMP packet comprises receiving an ICMP packet that specifies that fragmentation is needed (Talpade: [0020] lines 4-6: ICMP messages).

37. As per claim 32, Talpade as modified discloses the network element of claim 28. Talpade as modified further discloses wherein the step of authenticating the ICMP packet by determining if the packet sequence value is valid comprises determining if the packet sequence value is within a range of packet sequence values that are allowed by the transport protocol for the connection (Fan: column 10 lines 27-51).

38. As per claim 33, Talpade as modified discloses the network element of claim 28. Talpade as modified further discloses wherein the step of authenticating the ICMP packet by determining if the packet sequence value is valid comprises determining if the packet sequence value is within a range of sent but unacknowledged TCP packet sequence values for the connection (Fan: column 10 lines 27-51).

39. As per claim 34, Talpade as modified discloses the network element of claim 28. Talpade as modified further discloses wherein the step of authenticating the ICMP packet by determining if the packet sequence value is valid comprises determining if the packet sequence value is exactly equal to one or more sequence values of one or more packets that are then-currently

Art Unit: 2131

stored in a TCP re-transmission buffer, starting at a sequence value of a previously sent segment that resulted in receiving the ICMP packet (Fan: column 10 lines 35-41).

40. As per claim 35, Talpade as modified discloses the network element of claim 28. Talpade as modified further discloses wherein the steps are performed in a router acting as a TCP endpoint node (Talpade: [0020]: sensor/firewall).

41. As per claim 36, Talpade as modified discloses the network element of claim 28. Talpade as modified further discloses wherein the steps are performed in a firewall device (Talpade: [0020]: packet filtering device/firewall; Fan: column 10 lines 27-51: firewall/packet filter).

Response to Arguments

42. Applicant's arguments filed on 6/30/08 have been fully considered but they are not persuasive.

Regarding applicant's remarks, applicant argues that the prior art of record does not explicitly disclose authenticating ICMP packets by determining validity of values found within ICMP data fields. However, as indicated in the 35 U.S.C 112 rejection stated above, the support for amendment to the claims (Specification: [0012] and [0020]) does not constitute sufficient description reasonably convey that applicant had possession of the claimed invention when paragraph [0012] provides disclosure of prior art method and some well known format. Therefore, applicant's argument regarding the limitation is moot because the limitation raises an issue of new matter that is not considered by the examiner.

Art Unit: 2131

On the other hand, applicant argues that the prior art of record does not explicitly disclose updating a maximum transmission unit value associated with the TCP connection only if the packet sequence number is determined to be valid. However, the examiner has provided rationale in the above 35 U.S.C. 103 rejection to state that even although the particular method of allowing traffic flow is not specifically disclosed by the prior art of record (Talpade), Talpade discloses forwarding traffic flow when a field value is determined to be valid (Talpade: [0017] lines 28-30) and it would have been obvious to one having ordinary skill in the art to allow traffic flow by updating MTU value because allocating MTU for network traffic is well known in the art. Therefore, applicant's argument is traversed in light of above explanation.

Conclusion

43. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Art Unit: 2131

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shin-Hon Chen whose telephone number is (571) 272-3789. The examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Shin-Hon Chen/
Examiner, Art Unit 2131

Shin-Hon Chen
Examiner
Art Unit 2131